09-06-00.

A

09/05/00

JC905 U.S. PTO

JC813 U.S. PTO
09/655229
09/05/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

EL 596 028 545 US
"Express Mail" mailing Number

September 05, 2000
Date of Deposit

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above addressed to the

Commissioner of Patents and Trademarks
Washington, D.C. 20231

Marcelle Ivie

Marcelle Ivie

Law Office of Donald E. Schreiber
Post Office Box 64150
Sunnyvale, CA 94088-4150
(408) 541-9168

Dated: September 05, 2000

Applicant : Chung Nan Chang

Docket no. 2174

Serial No : (Unknown)

Filed : Herewith

For : SECURE CRYPTOGRAPHIC KEY EXCHANGE AND VERIFIABLE DIGITAL SIGNATURE

Commissioner of Patents
Washington, D.C. 20231

Transmitted herewith is a United States patent application entitled SECURE CRYPTOGRAPHIC KEY EXCHANGE AND VERIFIABLE DIGITAL SIGNATURE being filed in the name of Chung Nan Chang together with:

1. a Declaration, Power Of Attorney, And Petition For Patent Application executed by the inventor;
2. a Verified Statement (Declaration) Claiming Small Entity Status (37 CFR 1.9(f) and 1.27(b)) - Independent Inventor executed by the inventor;
3. a Verified Statement (Declaration) Claiming Small Entity Status (37 CFR 4.9(f) AND 4.27(c)) --Small Business Concern executed by an officer of the assignee of a fifty percent (50%) interest in the patent application; and

4. a $465.00 check in payment of the small entity United States patent application filing fee for an application with four (4) independent claims and a total of twenty-nine (29) claims.

The Commissioner of Patents and Trademarks is hereby authorized to charge any deficiency or credit any surplus in the patent application filing fee to Deposit Account No. 19-0735. A duplicate copy of this transmittal letter is enclosed herewith.

Donald E. Schreiber

Donald E. Schreiber
Reg. No. 29,435

Law Office of Donald E. Schreiber
Post Office Box 64150
Sunnyvale, California 94088-4150
(408) 541-9168

Dated: September 5, 2000

Applicant or Patentee: Chung Nan Chang
Serial or Patent No. (Unknown)
Filed or Issued Herewith
For SECURE CRYPTOGRAPHIC KEY EXCHANGE AND VERIFIABLE DIGITAL SIGNATURE

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY
STATUS (37 CFR 4.9(f) AND 4.27(b)) -- INDEPENDENT INVENTOR

As a below named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 CFR 4.9(c) for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code, to the Patent and Trademark Office with regard to the invention entitled SECURE CRYPTOGRAPHIC KEY EXCHANGE AND VERIFIABLE DIGITAL SIGNATURE
described in

[X] the specification filed herewith
[ ] application serial no. ______________, titled ______________
[ ] patent no. ______________, issues ______________

I have not assigned, granted, conveyed or licensed and am under no obligation under contract or law to assign, grant, convey or license, any rights in the invention to any person who could not be classified as an independent inventor under 37 CFR 4.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 4.9(d) or a nonprofit organization under 37 CFR 4.9(e).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

[ ] no such person, concern, or organization
[X] persons, concerns or organizations listed below*

*NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities.

(37 CFR 4.27)

FULL NAME On Line Post Corp
ADDRESS Fl. 12, No. 123, Sec. 2, Chung Hsiao E. Road, 100 Taipei, Taiwan R.O.C.
[ ] INDIVIDUAL [X] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

FULL NAME ______________
ADDRESS ______________
[ ] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

FULL NAME ______________
ADDRESS ______________
[ ] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

I hereby acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 4.28 (b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Chung Nan Chang		
NAME OF INVENTOR	NAME OF INVENTOR	NAME OF INVENTOR
Signature of Inventor	Signature of Inventor	Signature of Inventor
September 5, 2000		
Date	Date	Date

Applicant or Patentee: Chung Nan Chang

Serial or Patent No. (Unknown)

File or Issued Herewith

For SECURE CRYPTOGRAPHIC KEY EXCHANGE AND VERIFIABLE DIGITAL SIGNATURE

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS (37 CFR 4.9(f) AND 4.27(c)) -SMALL BUSINESS CONCERN

I hereby declare that I am

[ ] the owner of the small business concern identified below:

[X] an official of the small business concern empowered to act on behalf of the concern identified below :

NAME OF CONCERN On Line Post Corp.

ADDRESS OF CONCERN Fl. 12, No. 123, Sec. 2, Chung Hsiao E. Road

100 Taipei, Taiwan R.O.C.

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.3-18, and reproduced in 37 CFR 4.9(d). for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, entitled

SECURE CRYPTOGRAPHIC KEY EXCHANGE AND VERIFIABLE DIGITAL SIGNATURE

By inventor(s) Chung Nan Chang

described in

[X] the specification filed herewith

[ ] application serial no. ______________, filed ______________

[ ] patent no. ______________, issued ______________

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights to the invention is listed below* and no rights to the invention are held by and person, other than the inventor, who could not qualify as a small business concern under 37 CFR 4.9(d) or by any concern which would not qualify as a small business concern under 37 CFR 4.9(d) or a nonprofit organization under 37 CFR 4.9(e).

*NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities.

(37 CFR 4.27)

FULL NAME ______________________________

ADDRESS ______________________________

[ ] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

FULL NAME ______________________________

ADDRESS ______________________________

[ ] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

FULL NAME ______________________________

ADDRESS ______________________________

[ ] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 4.28 (b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING Tseng Chang Ching Lun

TITLE OF PERSON OTHER THAN OWNER President

ADDRESS OF PERSON SIGNING Fl.12, No.123, Sec.2, Chung Hsiao E. Road, Taipei, Taiwan, R.O.C.

SIGNATURE Tseng Chang Ching Lun DATE Aug. 30, 2000

SECURE CRYPTOGRAPHIC KEY EXCHANGE
AND VERIFIABLE DIGITAL SIGNATURE

Inventor: C. N. Chang

Attorney: Donald E. Schreiber
Law Office of Donald E. Schreiber
Post Office Box 61450
Sunnyvale, California 94088-4150

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates generally to cryptography and, more particularly, to exchanging cryptographic keys between two cryptographic units for a single cryptographic session, and to digital signature.

Description of the Prior Art

Two mutually-exclusive classes of cryptographic methods and protocols are well recognized by those familiar with cryptography, symmetric cryptography and public-key cryptography. In symmetric cryptographic protocols, the same key and cryptographic method are used both for encrypting a plaintext message into cyphertext, and for decrypting a cyphertext to recover the plaintext. It is readily apparent that the security of a symmetric cryptographic protocol can never exceed the security of the single key used both for encryption and decryption.

In conventional public-key cryptographic protocols there are two keys, a public key to which anyone can gain access and which is used only for encrypting a plaintext message, and a private key which only the recipient possesses and which is used only for decrypting a cyphertext. For such a public-key cryptographic protocol to be secure it must be unfeasible to determine the

private key by analyzing the public key. While public-key cryptographic systems appear alluring, thus far in practice it has been observed that public-key cryptographic methods are significantly slower than symmetric cryptographic methods. In general, it has been found that public-key cryptographic methods are 1000 times slower than symmetric cryptographic methods. Furthermore, present public key cryptographic methods rely upon difficult but solvable mathematical problems, e.g. factoring large integers or discrete logarithms. Such techniques, while providing some security, can be broken by a cryptanalytic attack that is less exhausting than a brute force attack.

Managing the distribution of cryptographic keys is the most difficult security problem in using cryptography both for symmetric protocols and for public-key protocols. Developing secure cryptographic methods and protocols is not easy, but making sure the keys used with such methods and protocols remain secret is an even more difficult task. "Cryptanalysts often attack both symmetric and public-key cryptosystems through their key management." Schneier, *Applied Cryptography*, Second Edition © 1996 Bruce Schneier ("Schneier") p. 169.

For symmetric cryptographic protocols, there are three well recognized key management problems. First, a key may be compromised which permits an eavesdropper who obtains the key either to read all the cyphertext, or even to broadcast bogus cyphertext.

The only way to alleviate this problem is to change keys frequently. A second problem for symmetric cryptography key management is that it requires a large number of keys if each pair of individuals in a group is to communicate using a different key. Forty-five unique keys are required if a group of 10 individuals are to communicate. Fifty-five unique keys are required for communication among a group of 11 individuals. The final problem for key management in symmetric cryptographic protocols is that, since keys are more valuable than the encrypted messages, the keys must be exchanged by a secure communication. One approach for securely distributing keys of a symmetric cryptographic protocol is to distribute them using a public-key cryptographic protocol.

Whether used with a symmetric cryptographic protocol or with a public-key cryptographic protocol, an encryption key should not be used indefinitely. First, the longer a key is used the more likely it will be compromised by theft, luck, extortion, bribery or cryptanalysis. Extended use of a key aids an eavesdropper because that provides more cyphertext encoded with the same key to which cryptoanalytic methods may be applied. Second, in general the longer a key is used the greater the loss if the key is compromised. Accordingly, it is not uncommon to encrypt each individual communication using a separate, session key that is used throughout only one particular communication session.

Schneier at pp. 41-68 provides an overview of protocols for

digital signatures, key exchange, and authentication. Schneier at pp. 513-522 describes in greater detail various key exchange protocols that may be used to establish a session key including:

1. Shamir's Three-Pass protocol which does not use any secret or public keys;
2. a COMSET protocol which uses a public key technique that is equivalent to factoring a large integer; and
3. an Encrypted Key Exchange ("EKE") protocol that may be implemented with various different cryptographic methods such as:
    a. a Rivest, Shamir and Adleman ("RSA") public-key cryptographic method that is described in United States patent no. 4,405,829;
    b. an ElGamal public-key cryptographic method; and
    c. a Diffie-Hellman public-key cryptographic method that is described in United States patent no. 4,200,770.

United States patent nos. 4,405,829 and 4,200,770 together with Schneier are hereby incorporated by reference.

While all of the preceding protocols provide some security for establishing a symmetric cryptographic key, the various protocols require exchanging several, time consuming communications between the parties to establish the key. Moreover, those protocols which require using a public-key cryptographic method also suffer from

the slowness of such methods. Furthermore, the preceding key exchange protocols are no more secure than the cryptographic method which they employed for key exchange, all of which can be broken by cryptanalysis that is less exhausting than a brute force attack.

Protocols for key exchange have been developed that are secure against all but a brute force cryptanalytic attack. United States Patent No. 5,583,939 ("the '939 patent") describes an exchange protocol which establish a session key useful for symmetric cryptography:

1. employing known and publicly identified mathematical functions; and
2. applied to exclusively private data, e.g. numbers.

In establishing this one-time key, an eavesdropper can learn both some of the numerical values selected by the parties in establishing the key, and also learn some of the numerical values computed using the known and publicly identified mathematical functions. The method disclosed in the '939 patent requires that the four known and publicly identified mathematical functions possess no inverse. That is, the four known and publicly identified functions must possess the property that knowing one of the quantities used in calculating a quantity and the calculated quantity, it is mathematically impossible to compute the other quantity used in performing the calculation. While the method disclosed in the '939 patent is swifter and simpler than previous methods, it requires

initially transmitting at least two quantities between the sender and the receiver, followed by a single quantity between the receiver and the sender.

Another United States Patent No. 5,987,130 ("the '130 patent") also describes an exchange protocol which establish a one-time key for use in symmetric cryptography:

1. employing known and publicly identified mathematical functions; and
2. applied to exclusively private data, i.e. numbers.

One of the ways in which the method for establishing a one-time key described in the '130 differs from that described in the '939 patent is that an eavesdropper cannot learn any numerical value selected by the parties in establishing the key. That is, the eavesdropper can learn only some of the numerical values computed using the known and publicly identified mathematical functions.

For the key exchange protocol described in the '130 patent a first of two cryptographic units "T" and "R" wishing to establish a cryptographic key "K" initially selects a first quantity "A". That same unit then uses a first mathematical function "Φ_1" and the selected quantity "A" to compute a second quantity "B" = $\Phi_1(A)$. The computed quantity B and the function Φ_1 must posses the property that knowing the computed quantity B, and the function Φ_1, it is mathematically impossible to compute the selected quantity A. That same unit then uses a second mathematical function "Φ_2" and

the selected quantity "A" to compute a third quantity "C" = $\Phi_2(A)$. The first unit T or R which selected the quantity A then transmits the computed quantity B to the other, second unit R or T, while retaining at the first unit T or R the computed quantity C.

Upon receiving the quantity B transmitted by the first unit T or R, the second unit R or T first selects a fourth quantity "D." Then using a third mathematical function Φ_3 together with the selected quantity D, the second unit T or R computes a fifth quantity "E" = $\Phi_3(D)$. The computed quantity E and the function Φ_3 must possess the property that knowing the computed quantity E, and the function Φ_3, it is mathematically impossible to compute the selected quantity D. That same unit then using a fourth mathematical function Φ_4 together with the selected quantity D computes a sixth quantity "F" = $\Phi_4(D)$. The second unit R or T which selected the quantity D then transmits the computed quantity E to the other, first unit T or R, while retaining at the second unit R or T the computed quantity F.

Then the second unit R or T uses a fifth mathematical function "Ψ_2" together with the calculated quantity F and the received quantity B to compute the key "K" = $\Psi_2(F, B) = \Psi_2(\Phi_4\{D\}, \Phi_1\{A\})$. The first unit T or R upon receiving the quantity E transmitted by the unit R or T then uses a sixth mathematical function Ψ_1 together with the calculated quantity C and the received quantity E to compute the key "K" = $\Psi_1(C, E) = \Psi_1(\Phi_2\{A\},\Phi_3\{D\}) = \Psi_2(\Phi_4\{D\},\Phi_1\{A\})$.

While the key exchange protocols disclosed both in the '939 and '130 patents permit establishing a session key for symmetric cryptography that an eavesdropper cannot crack except by using a brute force attack, it has not been possible to extend the disclosed techniques for use in digital signatures. The inability to extend the techniques disclosed in the '939 and '130 patents to digital signature appears to arise because the techniques disclosed there avoid using any pre-published, publicly available information in establishing the symmetric cryptographic key. Stated another way, while establishing the cryptographic key each party sends information to the other party on only one occasion, and therefor neither party publishes any information, other than the mathematical functions and the protocol for their use, before establishing the cryptographic key.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a cryptographic key exchange protocol which employs pre-established, publicly available information that is provably secure.

Another object of the present invention is to provide a cryptographic key exchange protocol that is faster than conventional protocols.

Another object of the present invention is to provide an encryption key exchange protocol that is secure against all but a

brute force cryptanalytic attack.

Another object of the present invention is to provide an improved, verifiable digital signature.

Another object of the present invention is to provide a digital signature that is secure against all but a brute force cryptanalytic attack.

Briefly, the present invention includes a protocol for cryptographic communication via a communication channel "I" in which a sending cryptographic unit "S" transmits onto the communication channel I an encrypted cyphertext message "M." The sending cryptographic unit "S" obtains the encrypted cyphertext message "M" by supplying both a plaintext message "P" and a cryptographic key "K" to a first cryptographic device. A receiving cryptographic unit "R" receives the cyphertext message M from the communication channel I, and supplies the cyphertext message M together with the key K to a second cryptographic device. The second cryptographic device decrypts the plaintext message P from cyphertext message M.

In one aspect, the present invention is a method by which the units S and R mutually establish a key K for a cryptographic session by first exchanging quantities before the sending unit S transmits the cyphertext message M. The method includes the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities. The sending unit S:

1. retrieves the plurality of public quantities from the

publicly accessible repository;

2. using at least some of the plurality of public quantities, computes and transmits to the receiving unit R a plurality of sender's quantities; and

3. using at least one of the plurality of public quantities, computes the session key K.

The receiving unit R, using at least one of the plurality of sender's quantities received from the sending unit S, computes the session key K.

In another aspect, the present invention is a protocol for communication in which a sending unit S transmits onto the communication channel I a message "M" together with a digital signature. However, before transmitting the message M and the digital signature, the sending unit S transmits for storage in the publicly accessible repository a plurality of public quantities. In the method of the present invention, a receiving unit R, that receives the message M and the digital signature, verifies the authenticity of digital signature as follows. The receiving unit R:

1. retrieves the plurality of public quantities from the publicly accessible repository;

2. using the digital signature and the plurality of public quantities, obtains at least two (2) results by evaluating expressions of at least two (2) different relation-

ships; and

3. compares both pairs of results obtained by evaluating the expressions of the at least two (2) different relationships.

Finding that the results obtained by evaluating the expressions for at least two (2) different relationships are equal verifies the digital signature.

These and other features, objects and advantages will be understood or apparent to those of ordinary skill in the art from the following detailed description of the preferred embodiment as illustrated in the drawing figure.

BRIEF DESCRIPTION OF THE DRAWING

FIG.1 is a block diagram depicting a cryptographic system which may be employed for secure cryptographic key exchange and digital signature via an insecure communication channel.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 illustrates a cryptographic system which may be employed for cryptographic key exchange that is referred to by the general reference character 10. The cryptographic system 10 includes a sender's cryptographic unit 12a, enclosed within a dashed line, and a receiver's cryptographic unit 12b, also enclosed within a dashed line. One particular unit has been assigned as the

sender's cryptographic unit 12a and another unit has been assigned as the receiver's cryptographic unit 12b only for pedagogical reasons. In principle, either unit could be the sender or the receiver. Each of the cryptographic units 12a and 12b respectively includes a cryptographic device 14. Each cryptographic device 14 includes a key input port 16, a plaintext port 18, and a cyphertext port 22.

The illustration of FIG. 1 depicts the cyphertext port 22 of the cryptographic device 14 included in the sender's cryptographic unit 12a as being coupled to a first input port 32 of a first transceiver 34a. Consequently, the cyphertext port 22 may supply a cyphertext message "M" to the first transceiver 34a. The first transceiver 34a also includes a first output port 36 from which the first transceiver 34a transmits the cyphertext message M via an insecure communication channel 38 to a first input port 32 of a second transceiver 34b. The insecure communication channel 38 may include a telephone link, a radio link, a microwave link, a coaxial cable link, a fiber optic link, or any other communication technology that permits transmitting data from a first location to a second location. Thus, for example, while an electronic or optical communication technology is presently preferred for the insecure communication channel 38, the insecure communication channel 38 might also include a messenger service, or a postal service. For a telephonic insecure communication channel 38, the

transceivers 34a and 34b might each respectively be conventional modems. Upon receipt of the cyphertext message M at the first input port 32 of the second transceiver 34b, the second transceiver 34b transmits the cyphertext message M from a first output port 36 to the cyphertext port 22 of the cryptographic device 14 included in the receiver's cryptographic unit 12b.

Arranged as described above and as illustrated in FIG. 1, the cryptographic units 12a and 12b provide a cryptographic system 10 in which a plaintext message P may be:

1. presented to the plaintext port 18 of the cryptographic device 14 included in the sender's cryptographic unit 12a;
2. encrypted by the cryptographic device 14 into the cyphertext message M;
3. transmitted from the cyphertext port 22 of the cryptographic device 14 via:
    a. the first transceiver 34a;
    b. the insecure communication channel 38; and
    c. the second transceiver 34b

    to the cyphertext port 22 of the cryptographic device 14 of the receiver's cryptographic unit 12b;
4. decrypted by the cryptographic device 14 back into the plaintext message P; and
5. transmitted from the plaintext port 18 of the crypto-

graphic device 14 included in the receiver's cryptographic unit 12b.

Alternatively, though not illustrated in FIG. 1, the cryptographic system 10 could be arranged so the plaintext message P is transmitted as a cyphertext message M from the cryptographic unit 12b to the cryptographic unit 12a. To effect such a reverse transmission of the plaintext message P, the cyphertext port 22 of the cryptographic device 14 included in the cryptographic unit 12b would be coupled to a second input 42 of the second transceiver 34b rather than to its first output port 36. A second output 44 of the second transceiver 34b would then transmit the cyphertext message M via the insecure communication channel 38 to a second input 42 of the first transceiver 34a. A second output 44 of the first transceiver 34a, rather than its first input port 32, would then be coupled to the cyphertext port 22 of the cryptographic device 14 included in the cryptographic unit 12a. Accordingly, in principle the cryptographic system 10 illustrated in FIG. 1 is capable of being configured for cryptographic transmission of the plaintext message P either from the cryptographic unit 12a to the cryptographic unit 12b as depicted in FIG. 1, or from the cryptographic unit 12b to the cryptographic unit 12a.

The precise cyphertext message M transmitted between the cryptographic units 12a and 12b depends not only upon the plaintext message P, but also upon a particular cryptographic method employed

by the cryptographic device 14 for encryption and/or decryption, and upon a cryptographic key "K" respectively supplied to the key input port 16 of each cryptographic device 14. To supply a cryptographic key K to each cryptographic device 14, both cryptographic units 12a and 12b in accordance with the present invention respectively include a key generator 52 having a key output port 54 from which the key generator 52 transmits the cryptographic key K to the cryptographic device 14.

The cryptographic system 10 depicted in FIG. 1 employs a symmetric cryptographic method for encrypting the plaintext message P, and for decrypting the cyphertext message M. Accordingly, in the illustration of FIG. 1, the cryptographic key $K^{\sim}$ supplied by the key generator 52 to the cryptographic device 14 of the sender's cryptographic unit 12a is identical to the cryptographic key $K^{\sim}$ supplied by the key generator 52 to the cryptographic device 14 of the receiver's cryptographic unit 12b. Described below is the protocol by which the cryptographic units 12a and 12b may mutually establish a cryptographic key $K^{\sim}$ in accordance with the present invention by exchanging messages between the cryptographic units 12a and 12b via the first transceiver 34a, the insecure communication channel 38 and the second transceiver 34b.

Secure Key Exchange

To permit establishing a secure session key to be used during communication between the cryptographic units 12a and 12b, a quantity source 62 included in the receiver's cryptographic unit 12b first generates the following private quantities.

1. a first private, three-element vector $a = (a_1, a_2, a_3)$
2. a private, large integer l
3. a second private, three-element vector $e = (e_1, e_2, e_3)$

The quantity source 62 then transmits the vector *a*, the large integer l, and the vector *e* from a quantity output port 64 of the quantity source 62 to a quantity input port 65 of the key generator 52 included in the receiver's cryptographic unit 12b. The quantity source 62 then continues to generate and transmit to the key generator 52 the following single quantity.

4. a first three-element vector $\alpha = (\alpha_1, \alpha_2, \alpha_3)$

In addition to transmitting α to the key generator 52, the receiver's cryptographic unit 12b also transmits α from a publication port 66 of the quantity source 62 for storage in a public repository 67 from which anyone may retrieve it. Numbers in all the quantities listed above are all integers chosen from a finite number set that are preferably obtained using a random number generator. Furthermore, the vector items generated by the quantity source 62, i.e. *a*. *e* and α must be linearly independent.

After the key generator 52 receives the quantities *a*. l, *e* and

α, the key generator 52 computes and also transmits to the public repository 67 from a publication port 68 two (2) more quantities listed below.

5. a third three-element vector $P_1 = 1^{a \times (e + \alpha)}$

6. a fourth three-element vector $P_2 = 1^{e}$

When the sender's cryptographic unit 12a wants to establish a secure session cryptographic key K for communication with cryptographic unit 12b, the quantity source 62 of the cryptographic unit 12a generates a private, three-element vector $r = (r_1, r_2, r_3)$ of random integers chosen from a finite number set. The quantity source 62 transmits the vector r from the quantity output port 64 to the quantity input port 65 of the key generator 52. After the key generator 52 receives the vector r, the key generator 52 first retrieves from the public repository 67 through a public-key retrieval-port 69 the three (3) quantities stored there by the receiver's cryptographic unit 12b, i.e. α, P_1 and P_2. Having retrieved those three (3) quantities, the sender's cryptographic unit 12a then computes two vector (2) quantities listed below.

$$V_1 = \alpha \times r$$

$$V_2 = 1^{e \times r}$$

After computing the two vector quantities V_1 and V_2, the key generator 52 of the sender's cryptographic unit 12a then transmits them to the receiver's cryptographic unit 12b via an output port 72, the first transceiver 34a, insecure communication channel 38,

second transceiver 34b and an input port 74 of the key generator 52.

After the receiver's cryptographic unit 12b receives the vector quantities V_1 and V_2, the cryptographic units 12a and 12b then possess all the data needed to independently establish the session cryptographic key K. The receiver's cryptographic unit 12b computes the session cryptographic key K as follows.

$$K = 1^{a \cdot (\alpha \times r)} 1^{e \times r \cdot a}$$

The sender's cryptographic unit 12a computes the session cryptographic key K as follows.

$$K = 1^{a \times (e + \alpha) \cdot r}$$

Because the cryptographic system 10 includes the insecure communication channel 38, an eavesdropper 82, which is not included in the cryptographic system 10 and which is enclosed within a dashed line in FIG. 1, may receive all of the communications between the cryptographic units 12a and 12b. Furthermore, the eavesdropper 82 has access to the public quantities stored in the public repository 67. The eavesdropper 82 includes a cryptographic device 14 which is functionally identical to, and may in principle be the same as, the cryptographic device 14 included both in the cryptographic units 12a and 12b. Therefore, if the eavesdropper 82 were able to determine the cryptographic key K using a key cracker 84 (e.g. by applying an inverse function to the quantities communicated between cryptographic units 12a and 12b during key

exchange and/or to the public quantities stored in the public repository 67) and supply the cryptographic key K to a key input port 16 of the cryptographic device 14, the eavesdropper 82 could decrypt the cyphertext message M to read the plaintext message P. Furthermore, if the eavesdropper 82 possesses the cryptographic key K, the eavesdropper 82 could then also transmit bogus cyphertext message M either to the sender's cryptographic unit 12a, to the receiver's cryptographic unit 12b, or to both.

In 1826 Neils Henrik Abel proved that a general equation of fifth or higher order can not be express in terms of radicals. In other words, such an equation can not be solved using purely algebraic means. For the real number system, such an equation can be solved using complex numbers, or a numerical approximation. However, such techniques are inapplicable to discrete, finite number system used for cryptography.

(C.N., I have created the hypothetical text set forth in the following paragraph from the text in your August 12, 2000, facsimile. Please check its accuracy.)

Using all three (3) public quantities, i.e. 4, 5 and 6 above, stored in the public repository 67 by the cryptographic unit 12b and the two vector quantities V_1 and V_2 which the cryptographic unit 12a transmits to the cryptographic unit 12b, solving for **a**, one private quantities retained by cryptographic unit 12b, requires solving an equation that includes the vector expression **a** x (**a** x $\boldsymbol{\alpha}$). Expressing the equation that includes the expression **a** x (**a** x

$\boldsymbol{\alpha}$) as a set of simultaneous equations and eliminating any pair of the quantities a_1, a_2, and a_3 yields an 8th order polynomial in the remaining quantity. Since solving analytically for any of the quantities a_1, a_2, and a_3 requires solving an 8th order polynomial, there exists no analytic method for computing the private, three-element vector quantity $\boldsymbol{a}$ from the public and transmitted quantities.

Verifiable Digital Signature

The preceding key exchange protocol may be augmented with additional quantities that allow the cryptographic unit 12b to append verifiable digital signatures to transmitted messages. First, in addition to selecting private, three-element vector $\boldsymbol{a}$, the quantity source 62 of the cryptographic unit 12b also selects a large, private integer m that it provides to the key generator 52. The quantity source 62 then continues to generate and transmit to the key generator 52 a second large integer n. In addition to transmitting n to the key generator 52, the receiver's cryptographic unit 12b also transmits n from the publication port 66 of the quantity source 62 for storage in a public repository 67 from which anyone may retrieve it. Using the integer m, the key generator 52 then computes and transmits to the public repository 67 three (3) additional public vectors.

7. a fifth three-element vector $S_1 = \boldsymbol{a} \times (\boldsymbol{a} \times \boldsymbol{\alpha})$

8. a sixth three-element vector $S_2 = m^{a \times (a \times (a \times \alpha))}$

9. a seventh three-element vector

$$S_3 = m^{(a \cdot \alpha)\ (a \times (a \times \alpha))}$$

Having stored the vectors S_1, S_2 and S_3 in the public repository 67, the cryptographic unit 12b may then append a digital signature to a message, either the plaintext message P or the cyphertext message M, in the following way. Assuming that the cryptographic unit 12b wants to append a digital signature to the plaintext message P, it first hashes the message P to obtain a three element vector p. After establishing the vector p, the cryptographic unit 12b then appends to the plaintext message P as the digital signature the following three element vector.

$$m^{((a \cdot p)^\wedge n)\ a + a \times p}$$

After retrieving the public quantities that have been stored in the public repository 67, anyone receiving the plaintext message P to which the cryptographic unit 12b has appended the digital signature can verify the signature's authenticity by evaluating and comparing the two following verification expressions.

1. $m^{(((a \cdot p)^\wedge n)\ a + a \times p)\ \cdot\ a \times (a \times \alpha)}$

$$\stackrel{?}{=} m^{a \times (a \times (a \times \alpha))\ \cdot\ p}$$

2. $m^{(((a \cdot p)^\wedge n)\ a + a \times p)\ \cdot\ (a \times (a \times \alpha)) \times \alpha}$

$$\stackrel{?}{=} m^{-(a \cdot \alpha)\ a \times (a \times \alpha)\ \cdot\ p}$$

Finding that the quantities obtained by evaluating the two

expressions on both sides of the "$\stackrel{?}{=}$" in verification relationship no. 1 above are identical, and also finding that the quantities obtained by evaluating the two expressions on both sides of the "$\stackrel{?}{=}$" in verification relationship no. 2 above are identical, verifies the digital signature.

The first expression set forth above prevents a forger from appending a known quantity $m^{a \times p}$ to the plaintext message P as the signature. The second expression ensures that the cryptographic unit 12b has used the private vector *a* in computing the digital signature.

Considering the public non-linear quantity that includes the term $a \times (e \times a)$, solving for the private, three-element vector *a* requires finding the roots of at least an 8^{th} order polynomial. For the reason stated above, there exists no analytic method for finding the roots an 8^{th} order polynomial. Consequently, cryptanalysts can find the private, three-element vector *a* only by brute force.

There exist additional expressions which may be used to establish other verification relationships in addition to the two set forth above. However, two such verification relationships appear to be sufficient to ensure that the cryptographic unit 12b has appended the digital signature to the message.

Although the present invention has been described in terms of

the presently preferred embodiment, it is to be understood that such disclosure is purely illustrative and is not to be interpreted as limiting. For example, as those skilled in the art will understand, after the cryptographic units 12a and 12b have established the session key K in accordance with the present invention, either of the cryptographic units 12a or 12b may send or may receive cyphertext messages M_i from the other in any arbitrary order. Analogously, while the digital signature technique may be used with the plaintext message P, it may also be used to authenticate the cyphertext message M. Consequently, without departing from the spirit and scope of the invention, various alterations, modifications, and/or alternative applications of the invention will, no doubt, be suggested to those skilled in the art after having read the preceding disclosure. Accordingly, it is intended that the following claims be interpreted as encompassing all alterations, modifications, or alternative applications as fall within the true spirit and scope of the invention.

What Is Claimed Is:

1. In a protocol for cryptographic communication via a communication channel "I" in which a sending cryptographic unit "S" transmits onto the communication channel I an encrypted cyphertext message "M" obtained by supplying both a plaintext message "P" and a cryptographic key "K" to a first cryptographic device, and in which a receiving cryptographic unit "R" receives the cyphertext message M from the communication channel I and by supplying the cyphertext message M together with the key K to a second cryptographic device decrypts the plaintext message P therefrom, a method by which the units S and R mutually establish a cryptographic key K by first exchanging messages before the sending unit S transmits the cyphertext message M comprising the steps of:

a. the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities;

b. the sending unit S:

i. retrieving the plurality of public quantities from the publicly accessible repository;

ii. using at least some of the plurality of public quantities, computing and transmitting to the receiving unit R a plurality of sender's quantities; and

iii. using at least one of the plurality of public quantities, computing the key K; and

c. the receiving unit R, using at least one of the plurality of sender's quantities received from the sending unit S computing the key K.

2. The method of claim 1 wherein the receiving unit R, in storing the plurality of public quantities into the publicly accessible repository:

i. selects at least one receiver's secret quantity;

ii. selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity; and

iii. using the receiver's secret quantity and the at least one selected public quantity, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities.

3. The method of claim 2 wherein the plurality of public quantities include a plurality of vectors.

4. The method of claim 2 wherein the at least one selected

public quantity includes a vector.

5. The method of claim 2 wherein the plurality of computed public quantities include a plurality of vectors.

6. The method of claim 2 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R:

i. selects a sender's secret quantity; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit R the plurality of sender's quantities.

7. The method of claim 6 wherein the plurality of sender's quantities include a plurality of vectors.

8. The method of claim 1 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R:

i. selects a sender's secret quantity; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public

quantities, computes for transmission to the receiving unit R the plurality of sender's quantities.

9. The method of claim 8 wherein the plurality of sender's quantities include a plurality of vectors.

10. A system adapted for communicating as an encrypted cyphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system comprising:

a. a communication channel I adapted for transmitting the cyphertext message M;

b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the cyphertext message M from one transceiver to the other transceiver via said communication channel I; and

c. a pair of cryptographic units each of which is respectively coupled to one of said transceivers for transmitting the cyphertext message M thereto or receiving the cyphertext message M therefrom, each cryptographic unit:

i. when the cryptographic unit is to receive the cyphertext message M:

(1) storing plurality of public quantities in a publicly accessible repository;

(2) receiving via the communication channel I a plurality of sender's quantities from a sending cryptographic unit, and using at least one of the plurality of sender's quantities in computing the key K; and

ii. when the cryptographic unit is to send the cyphertext message M, retrieving the plurality of public quantities from the publicly accessible repository and using:

(1) at least some of the plurality of public quantities in computing the plurality of sender's quantities which the sending cryptographic unit transmits via the communication channel I to the receiving cryptographic unit; and

(2) at least one of the plurality of public quantities in computing the key K; and

iii. including a cryptographic device having:

(1) a key input port for receiving the key K from the cryptographic unit;

(2) a plaintext port:

(a) for accepting the plaintext message P for

encryption into the cyphertext message M that is transmitted from the cryptographic device, and

(b) for delivering the plaintext message P obtained by decrypting the cyphertext message M received by the cryptographic device; and

(3) a cyphertext port that is coupled to one of said transceivers:

(a) for transmitting the cyphertext message M to such transceiver, and

(b) for receiving the cyphertext message M from such transceiver.

11. The system of claim 10 wherein said cryptographic unit which receives the cyphertext message M in storing the plurality of public quantities into the publicly accessible repository:

(a) selects at least one receiver's secret quantity;

(b) selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity; and

(c) using the receiver's secret quantity and the at least one selected public quantity, computes and

stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities.

12. The system of claim 11 wherein the plurality of public quantities include a plurality of vectors.

13. The system of claim 11 wherein the at least one selected public quantity includes a vector.

14. The system of claim 11 wherein the plurality of computed public quantities include a plurality of vectors.

15. The system of claim 11 wherein the sending cryptographic unit, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit::

i. selects a sender's secret quantity;; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

16. The system of claim 15 wherein the plurality of sender's

quantities include a plurality of vectors.

17. The system of claim 10 wherein the sending cryptographic unit, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

i. selects a sender's secret quantity;; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

18. The system of claim 17 wherein the plurality of sender's quantities include a plurality of vectors.

19. A cryptographic unit adapted for inclusion in a system for communicating as an encrypted cyphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system including:

a. a communication channel I adapted for transmitting the cyphertext message M; and

b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the cyphertext message M from one

transceiver to the other transceiver via said communication channel I;

the cryptographic unit being adapted for coupling to said transceivers for transmitting the cyphertext message M thereto or receiving the cyphertext message M therefrom, and comprising:

a. ports:

i. when the cryptographic unit is to receive the cyphertext message M, for:

(1) storing plurality of public quantities in a publicly accessible repository;

(2) receiving via the communication channel I a plurality of sender's quantities from a sending cryptographic unit, and using at least one of the plurality of sender's quantities in computing the key K; and

ii. when the cryptographic unit is to send the cyphertext message M, for retrieving the plurality of public quantities from the publicly accessible repository and using:

(1) at least some of the plurality of public quantities in computing the plurality of sender's quantities which the sending cryptographic unit transmits via the communication channel I to the receiving

cryptographic unit; and

(2) at least one of the plurality of public quantities in computing the key K; and

b. a cryptographic device having:

i. a key input port for receiving the key K from the cryptographic unit;

ii. a plaintext port:

(1) for accepting the plaintext message P for encryption into the cyphertext message M that is transmitted from the cryptographic device, and

(2) for delivering the plaintext message P obtained by decrypting the cyphertext message M received by the cryptographic device; and

ii. a cyphertext port that is coupled to one of said transceivers:

(1) for transmitting the cyphertext message M to such transceiver, and

(2) for receiving the cyphertext message M from such transceiver.

20. The cryptographic unit of claim 19 wherein, when receiving the cyphertext message M, in storing the plurality of public quantities into the publicly accessible repository:

(a) selects at least one receiver's secret quantity;

(b) selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity; and

(c) using the receiver's secret quantity and the at least one selected public quantity, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities.

21. The cryptographic unit of claim 20 wherein the plurality of public quantities include a plurality of vectors.

22. The cryptographic unit of claim 20 wherein the at least one selected public quantity includes a vector.

23. The cryptographic unit of claim 20 wherein the plurality of computed public quantities include a plurality of vectors.

24. The cryptographic unit of claim 20, when sending the cyphertext message M, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

i. selects a sender's secret quantity; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

25. The cryptographic unit of claim 24 wherein the plurality of sender's quantities include a plurality of vectors.

26. The cryptographic unit of claim 19 wherein, when sending the cyphertext message M, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

i. selects a sender's secret quantity; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

27. The cryptographic unit of claim 26 wherein the plurality of sender's quantities include a plurality of vectors.

28. In a protocol for communication in which a sending unit S transmits onto the communication channel I a message "M" together

with a digital signature, and, wherein before transmitting the message M and the digital signature, the sending unit S transmits for storage in a publicly accessible repository a plurality of public quantities, a method by which a receiving unit R that receives the message M and the digital signature verifies the authenticity of digital signature comprising the steps performed by the receiving unit R of:

a. retrieving the plurality of public quantities from the publicly accessible repository;

b. using the digital signature and the plurality of public quantities, evaluating expressions of at least two (2) different verification relationships; and

c. comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

29. The method of claim 28 wherein the plurality of public quantities include a plurality of vectors.

ABSTRACT

One aspect of the present invention establishes a session key by a receiving unit R transmitting a plurality of quantities for storage in a public repository. A sending unit S:

1. retrieves the plurality of quantities; and
2. computes and transmits to the unit R a plurality of sender's quantities; and
3. using at least one of the plurality of public quantities, computes the session key K.

The unit R, using the sender's quantities:

1. computes and transmits to the unit S at least one receiver's quantity; and
2. computes the session key.

Another aspect provides a digital signature. Before transmitting a signed message, the unit S stores a plurality of quantities in the public repository. A unit R, that receives the message and the digital signature, verifies their authenticity by:

1. retrieving the quantities from the repository;
2. using the digital signature and the quantities, evaluates expressions in at least two (2) different relationships; and
3. verifies the digital signature upon finding equality between evaluation results.

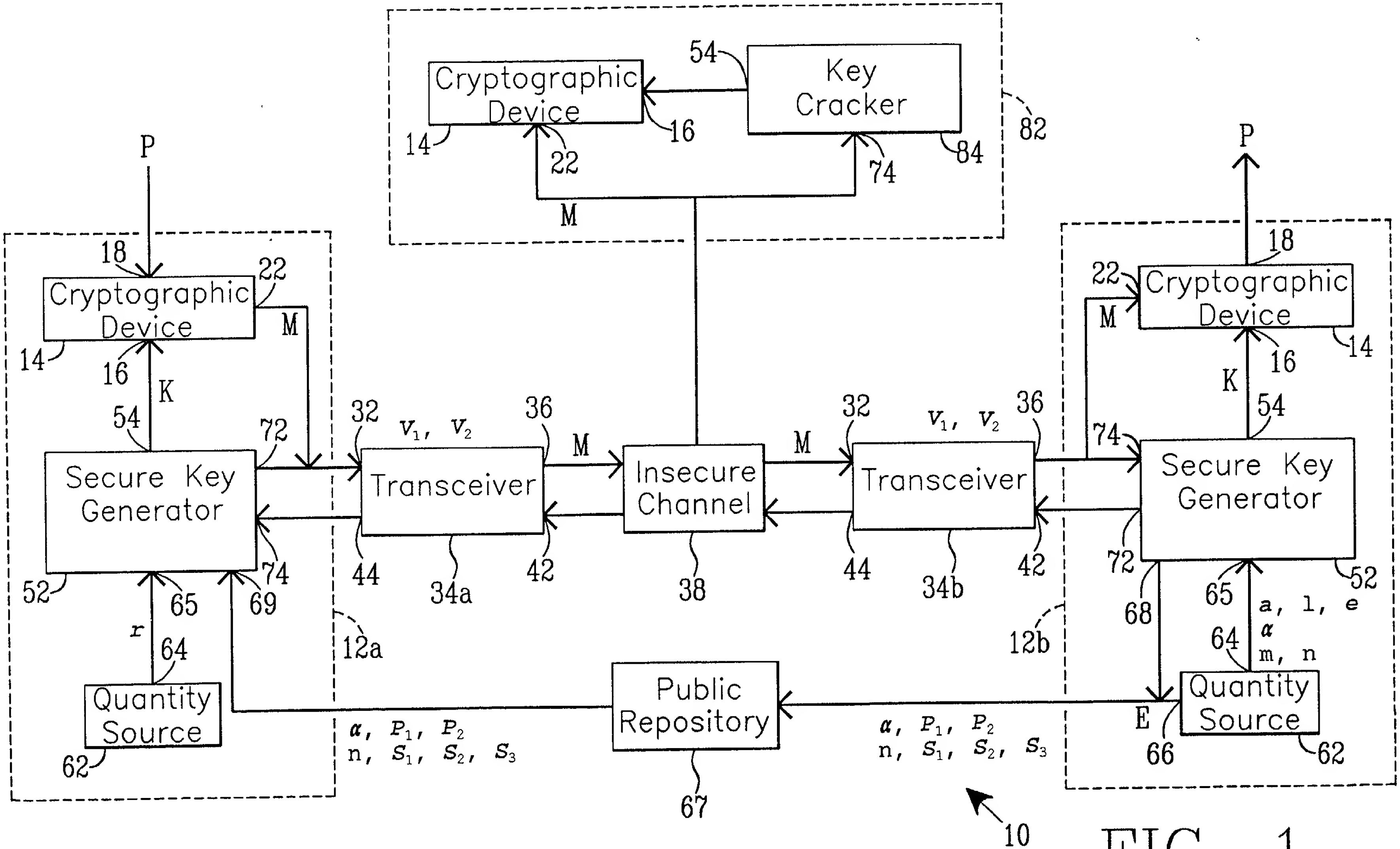
Cryptographic Device
Key Cracker
54
14
16
22
74
84
82
M
P
18
22
Cryptographic Device
14
16
K
54
72
M
Secure Key Generator
52
65
69
74
r
64
Quantity Source
62
12a
32
v_1, v_2
36
Transceiver
44
34a
42
M
Insecure Channel
38
M
32
v_1, v_2
36
Transceiver
44
34b
42
12b
P
18
22
M
Cryptographic Device
14
16
K
54
74
Secure Key Generator
72
52
68
65
a, l, e
α
m, n
64
Quantity Source
E
66
62
Public Repository
67
α, P_1, P_2
n, S_1, S_2, S_3
α, P_1, P_2
n, S_1, S_2, S_3
10

FIG. 1

DOCKET NO. 2174

DECLARATION, POWER OF ATTORNEY, AND PETITION
FOR PATENT APPLICATION

As an inventor identified below, I hereby declare that:

My residence, citizenship, and residence address are as stated below beneath my name;

I believe I am the original, first, and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

SECURE CRYPTOGRAPHIC KEY EXCHANGE
AND VERIFIABLE DIGITAL SIGNATURE

described and claimed in the accompanying specification.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims.

In accordance with Title 37, Code of Federal Regulations, § 1.56(a), I acknowledge my duty to disclose all information known to me which is material to the examination of this application.

I do not know and do not believe that the invention described and claimed in this application was:

> Known or used in the United States of America before my invention thereof, or patented or described in a printed publication in any country before my invention thereof; or
>
> Patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the filing date of the present patent application in the United States of America; or
>
> First patented or caused to be patented, or was the subject of an inventor's certificate by me or my legal representative(s) or assign(s) in a foreign country prior to the date of the filing date of the application for patent in this country on an application for patent or inventor's certificate filed more than twelve months before the filing date of the application in the United States of America; or
>
> Described in a patent granted on an application for patent by another filed in the United States of America before the invention thereof by me, or on an international application by another who has fulfilled the requirements of

the first, second, and fourth paragraphs of Title 35, United States Code, § 371(c) before my invention thereof.

The undersigned hereby appoints Donald E. Schreiber, Post Office Box 64150, Sunnyvale, California 94088-4150, Registration No. 29,435, his attorney to prosecute this application for letters patent, with full power of substitution and revocation, to transact all business in the Patent and Trademark Office in connection therewith, and to receive any patent issuing thereon.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, § 1001, and that such willful false statements may jeopardize the validity of the present application or any patent issued thereon.

Wherefore, I pray that Letters Patent be granted to me for the invention described and claimed in the accompanying specification and claims, and I hereby subscribe my name to the accompanying specification and claims, and the foregoing declaration, power of attorney, and petition.

Chung Nan Chang

Residence: United States of America

Citizenship: United States of America

Residence Address:
1455 Wessex Avenue
Los Altos, California
95024